UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/021,268	12/07/2001	Itzhak I. Rubinstein	3127.1000-004	9770

21005 7590 08/25/2005

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

EXAMINER	
POLTORAK, PIOTR	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/021,268	RUBINSTEIN ET AL.	
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 5-29-02
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-26 have been examined.

Priority

2. Acknowledgment is made of applicant's claim for priority based on U.S. Provisional Application No. 60/254,460, filed on Dec. 8, 2000 and on a continuation-in-part of U.S. application Ser. No. 09/182,154, filed Oct. 29, 1998, which claims the benefit of U.S. Provisional Application No. 60/063,919, filed on Oct. 31, 1997,

Claim Objections

3. "A initialization string" in claims 1, 5, 9, 13, 18 and 21 should be "an initialization string".
4. Claim 5 should be rewritten in order to clarify limitation (c), e.g. by changing "comprising" to "using". Similarly applicant should clarify claim 9 (f).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.
6. "The next block of data" in claims 1, 5, 9 and 13 lacks antecedent basis.
7. "Sender" and "receiver" lack antecedent basis in claims 1-26.

8. Claims 1-26 are ambiguous due to the complex language used in constructing the claim limitations. In particular the phrase: "calculating synchronization data at sender and receiver by pseudo-random function means operating on data comprising the current data block" in claim 2 does not allow to draw a clear interpretation. It is not clear whether "comprising the current data block" refers to the "pseudo-random function means operating on data" or whether it refers to the "synchronization data". Another example: "generating a new encryption key by pseudo-random-function means operating on data comprising the previous intermediate keys" does not allow one to ascertain whether it is "the new encryption key" or "the data" that comprise the previous intermediate keys. Applicant should check all the claims for similar variation of cited ambiguities.
9. Claim 1 recites "repeating the steps from (d) forward repeatedly until the data is exhausted". The limitation is not understood. Repeating the steps from (d) does not make much sense: either there is a missing step, or the repeating steps should start from (c), or generating a new encryption key in step (f) is unnecessary.
   The examiner assumes that the newly generated encryption keys are for encrypting the next block of data and as a result lines 19-20 of pg. 22 should read "repeating the steps from (c) forward repeatedly until the data is exhausted".
10. A missing step is also observed in claim 5.
11. Claim 5 (f) is not understood. It is not clear whether the initialization string is included in the data or it is simply used in generating a new encryption key.

The examiner assumes that applicant meant generating a new encryption key using the initialization string.

12. A similar problem has been observed in claim 9, which for purposes of further examination is similarly treated as mentioned above *(the previous §)*.

13. Claim 13 (d) specifies generating one or more second keys (permitting generation of just one key) but following step 13 (f) specifies generating an encryption key using the second intermediate keys at both the sender and the receiver. The claim limitations are treated as best understood.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

14. Claims 18-19 are rejected under 35 U.S.C. 102(b) as anticipated by *Jones (U.S. Patent No. 5412730)*.

15. *Jones* teaches (a) exchanging an initialization string by secure, external means between sender and receiver *(col. 4 lines 15-20)*; (b) generating an encryption key by pseudo-random-function means operating on data comprising the initialization

string at both the sender and the receiver *(col. 3 lines 26-29 and Fig. 1)*; and (c) repeating the steps from (b) forward when signaled by the host software *(col. 3 lines 33-40)*.

Claim Rejections - 35 USC § 102 or 103

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. Claim 5 is rejected under 35 U.S.C. 102(b) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over *Jones (U.S. Patent No. 5412730)*.

17. As per claim 5 *Jones* teaches (a) exchanging an initialization string by secure, external transmission between sender and receiver *(col. 4 lines 15-20)*; (b) generating an encryption key by pseudo-random-function means operating on data comprising the initialization string at both sender and receiver *(encryption key, col. 3 lines 26-29 and Fig. 1)*; (c) encrypting the next block of data into ciphertext by symmetric-key-encryption algorithm means comprising the encryption key at the sender *(col. 3 lines 28-29 and lines 11-13)*; (d) transmitting the ciphertext to the

receiver *(col. 3 lines 57-58)*; (e) decrypting the ciphertext by symmetric-key-encryption algorithm means comprising the encryption key at the receiver *(col.3 lines 57-62)*; and (f) generating a new encryption key at both sender and receiver by pseudo-random-function means operating on data comprising the initialization string *(col. 3 lines 30-33)*;

18. *Jones* does not explicitly teach repeating the steps from (d) forward repeatedly until the data is exhausted. However, *Jones* teaches repeating the steps from (d) forward *(col. 3 lines 13-25 and 26-40)* and the examiner believes that such a repetition would have been conducted until the data is exhausted. Even if the repetition as taught by *Jones* would not have been conducted until the data is exhausted it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement such a modification. One of ordinary skill in the art would have been motivated to perform such a modification in order to keep all of the data blocks secure.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 1-4, 6-17, 20-23 are rejected under 35 U.S.C. 103(a) as obvious over *Jones (U.S. Patent No. 5412730)* in view of *Schneier (Bruce Schneier, "Applied*

Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457).

20. *Jones* teaches the method as discussed above.

21. As per claim 1 *Jones* does not teach that a new encryption key is generated comprising the previous encryption key.

22. *Schneier* teaches that a new encryption key is generated comprising the previous encryption key *(Schneier, 8.6 Updating keys, pg. 180).*

23. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize a previous encryption key in generation of a new encryption key. One of ordinary skill in the art would have been motivated to perform such a modification in order to increase security.

24. Claims 9, 13 and 21 are essentially the same as claim 1with only one notable difference: a number of keys being used in the process of generating the key used in encrypting data. Althought on pg. 180 *Schneier* does not explicitly spell out that multiple keys can be used in "key updating", *Schneier* discloses the feature of deriving an encryption key from multiple keys in Fig. 12.1 on pg. 271.
It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use a number of keys in the process of generating the key used in encrypting data as taught by *Schneier* for given the motivation of increased security.

25. *Jones* in view of *Schneier* teach the pseudo-random function means operating on data comprising the current data block as discussed above.

26. As per claims 2, 6, 10, 14, 20 and 23 *Jones* in view of *Schneier* do not teach calculating synchronization data at the sender and the receiver by pseudo-random function means operating on data comprising the current data block; including the synchronization data with the ciphertext transmitted to the receiver; comparing the synchronization data received with the synchronization calculated; signaling resynchronization requests from receiver to sender; acknowledging resynchronization requests; and re-executing the steps of the claim from the appropriate step forward.

27. Official Notice is taken that it is old and well-known practice to synchronize data at the sender and the receiver. One of ordinary skill in the art at the time of applicant's invention would have been motivated to employ synchronization of data at the sender and the receiver to assure correct data transfer *(e.g. Malter, U.S. Patent No. 4860323, Fig. 5-A-C, col. 3 lines 23-28, Aslanis et al., U.S. Pub. 20020094049, [10] etc.)*.

28. Comparing the synchronization data received with the synchronization calculated is implicit.

29. It is similarly well-known practice to signal resynchronization requests from the receiver to the sender and acknowledging the requests. In addition one of ordinary skill in the art at the time of applicant's invention would have been motivated to employ signaling the resynchronization requests from the receiver to the sender and acknowledging requests in order to recover from errors occurring in data communication *(e.g. Botrel et al., U.S. Patent No. 4551839, col. 9 lines 61-62)*.

30. Re-executing the steps of the claim from the appropriate step forward would be implicit.

31. *Schneier's* teaching *(Fig. 12.1)* reads on claim 4, 8, 12 and 16-17.

32. Claims 24-26 are rejected under 35 U.S.C. 103(a) as obvious over *Jones (U.S. Patent No. 5412730)* in view of *Schneier (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457)* and in further view of *Malter (U.S. Patent No. 4860323)* and in further view of *Kaufman et al. (Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security, Private communication in a Public World 1995, ISBN: 0130614661).*

33. *Jones* in view of *Schneier* teach operating on data comprising the initialization string at both the sender and the receiver as discussed above.

34. *Jones* in view of *Schneier* do not teach generating an authentication code by function means operating on data comprising the initialization string at both the sender and the receiver; transmitting the authentication code from the sender to the receiver, said code constituting a remote code at the receiver; transmitting the authentication code from receiver to sender, said code constituting a remote code at the sender; comparing the remote code to the generated code at both the sender and the receiver.

35. *Kaufman et al.* teach generating an authentication code at both sender and receiver, transmitting the authentication code from sender to receiver, said code constituting a remote code at the receiver; comparing the remote code to the generated code at both sender and receiver *(9.2.3 Public Keys, pg. 236).*

36. *Jones* in view of *Kaufman et al.* do not teach transmitting an authentication error from the receiver to the sender when the receiver remote code does not correspond to the receiver generated code and transmitting an authentication error from the sender to the receiver when the sender remote code does not correspond to the sender generated code.

37. Official Notice is taken that it is old and well-known practice to transmit an authentication error from one party to another when the generated remote code does not correspond to the received generated code *(e.g. Windows NT domain authentication)*. One of ordinary skill in the art at the time of applicant's invention would have been motivated to transmit an authentication error from one party to another when the generated remote code does not correspond to the received generated code in order to alert the authenticated party about the error.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Signature

8/21/05

Date

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100